

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

TREND MICRO, INC.,
Petitioner,

v.

TAASERA LICENSING LLC,
Patent Owner.

IPR2023-00800
Patent 8,990,948 B2

Before NEIL T. POWELL, KRISTIL R. SAWERT, and
SCOTT RAEVSKY, *Administrative Patent Judges*.

POWELL, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

A. BACKGROUND

Trend Micro Inc. (“Petitioner”) filed a Petition (Paper 2 (“Pet.”)) requesting an *inter partes* review of claims 1–5 of U.S. Patent No. 8,990,948 B2 (Ex. 1001, “the ’948 patent”). Taasera Licensing LLC (“Patent Owner”) filed a Preliminary Response. Paper 6 (“Prelim. Resp.”).

An *inter partes* review may not be instituted “unless . . . the information presented in the petition . . . shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” 35 U.S.C. § 314(a). Having considered the arguments and the associated evidence, we determine that Petitioner has not shown a reasonable likelihood that it will prevail in establishing the unpatentability of any of the challenged claims. Accordingly, we do not institute *inter partes* review.

B. RELATED PROCEEDINGS

The parties note that the ’948 patent has been asserted in *In re Taasera Licensing, LLC, Patent Litigation*, MDL No. 3042, consolidated as 2:22-md-03042 (E.D. Tex.). Pet. 74; Paper 3, 2. Petitioner also identifies IPR2023-00799 as involving a related patent (U.S. Patent No. 9,092,616). Pet. 74. Patent Owner also identifies the following related district court proceedings: *Taasera Licensing LLC v. Trend Micro Inc.*, No. 2:21-cv-00441-JRG (E.D. Tex.); *Taasera Licensing LLC v. Check Point Software Techs. Ltd.*, No. 2:22-cv-00063-JRG (E.D. Tex.); *Trend Micro Inc. v. Taasera Licensing LLC*, No. 2:22-cv-00303-JRG (E.D. Tex.); *Palo Alto Networks, Inc. v. Taasera Licensing LLC*, No. 2:22-cv-00314-JRG (E.D. Tex.); *Taasera Licensing LLC v. Fortinet Inc.*, No. 2:22-cv-00415-JRG

(E.D. Tex.); *Taasera Licensing LLC v. Musarubra US LLC, d/b/a Trellex*, No. 2:22-cv-00427-JRG (E.D. Tex.); and *Taasera Licensing LLC v. CrowdStrike, Inc., et al.*, No. 2:22-cv-00468-JRG (E.D. Tex.). Paper 3, 2–3. Additionally, Patent Owner identifies IPR2023-00705 as a related matter. Paper 3, 2.

C. REAL PARTIES-IN-INTEREST

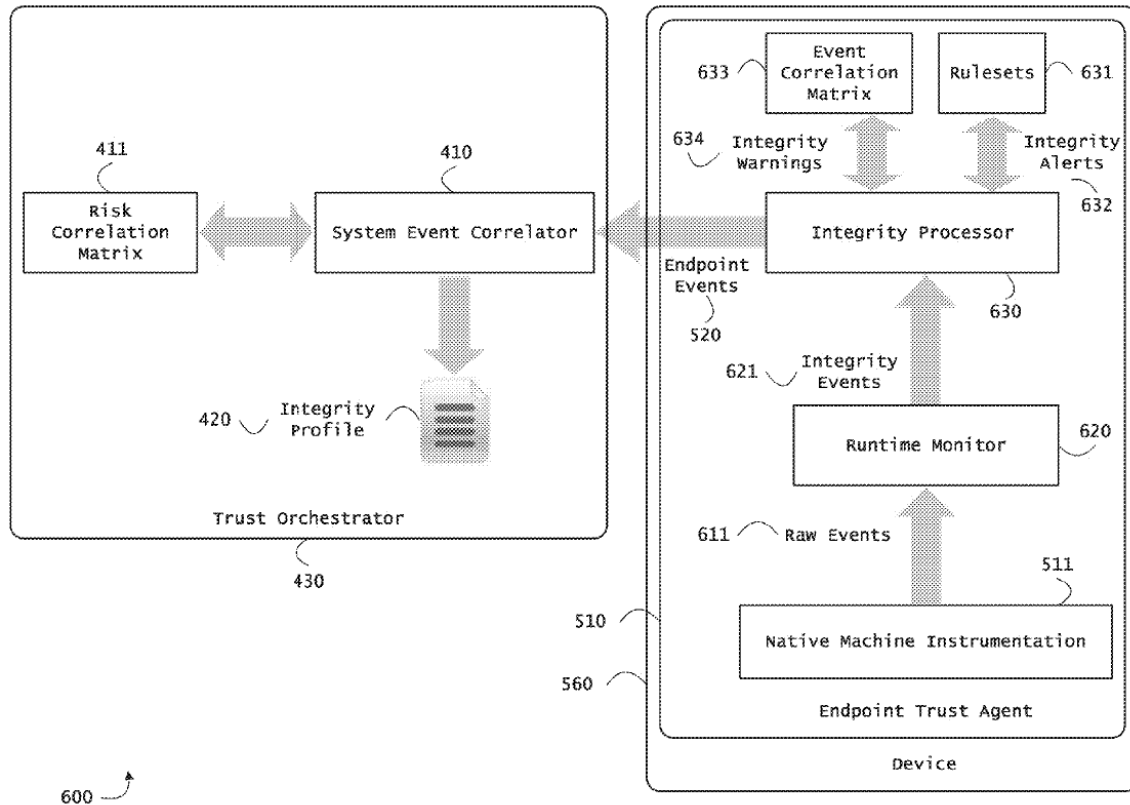
Petitioner identifies the following real-parties-in interest: “Trend Micro, Inc., Trend Micro America, Inc. and Trend Micro Incorporated.” Pet. 73. Patent Owner states that “[t]he patent owner and real party-in-interest is Taasera Licensing LLC.” Paper 3, 2.

D. THE ’948 PATENT

The ’948 patent relates to data center virtualization. Ex. 1001, 1:15–26. According to the ’948 patent, “virtualized, cloud computing on-demand, and elastic models require dynamic security orchestration at both the device and network level that is lacking in traditional security approaches and technologies.” *Id.* at 2:2–6. The ’948 patent explains that its “presently disclosed exemplary technical solutions may be embodied as a method, apparatus and/or system for integrity confidence measurement.”

Id. at 5:59–61. The '948 patent discusses one embodiment in connection with Figure 6, which is reproduced below.

FIG. 6



“[Figure] 6 depicts data flows between components of an exemplary system for correlating endpoint events.” *Id.* at 15:2–3.

In particular, Figure 6 shows data flows within correlation system 600. *Id.* at 15:3–6. “[C]orrelation system 600 includes an endpoint trust agent 510 on a device 560.” *Id.* at 15:10–11. Endpoint trust agent 510 includes runtime monitor 620, which is “configured to register for and receive a plurality of raw events 611 from native machine instrumentation 511 on the device 560” and to “raise integrity events 621 to an integrity processor 630.” *Id.* at 15:11–16, 15:20–22. Integrity processor 630 “may apply rulesets 631 to generate integrity alerts 632 and generate or populate an event correlation matrix 633 that maps integrity

warnings 634 to endpoint events 520 for dispatch to a trust orchestrator 430.” *Id.* at 15:16–19.

“[T]rust orchestrator 430 comprises a system event correlator 410 configured to use a risk correlation matrix 411 to generate an integrity profile 420 for the monitored system.” *Id.* at 15:30–33. “In one embodiment, the system event correlator 410 can be implemented as a correlation engine.” *Id.* at 15:33–35. “For the risk correlation matrix 411 shown in FIG. 6, each cell in the grid is a set of alerts triggered through an event correlation matrix 633 and rulesets 631 (rule expressions) by the endpoint trust agent 510.” *Id.* at 15:38–41.

The ’948 patent further discusses an embodiment of a risk correlation matrix in connection with Figure 7C, which is reproduced below.

FIG. 7C

VM UUID	S1	S2	S3	S4
56 4d ef 2d 3f d4 14 e2-2e 04 c5 34 3a ec ee 65	P ₁ ... P ₄		A ₄ ... A ₆	
65 4d 2f 2d 3f d4 41 e2-2e 04 c5 34 3a ec ee ef		P ₃ ... P ₇	A ₃ ... P ₄	I ₂ ... I ₉
34 5d cf 2d 1f d4 14 e2-2e 04 c5 34 3b ec ee de		P ₁₁		
51 4d ef 2d 3f e4 24 c2-2e 04 c5 34 3a ec ee 23	P ₇ ... P ₁₀	P ₄	P ₃ ... A ₉	G ₄ ... G ₉
.				I ₇ ... G ₁₀
25 d4 ef d2 3f d4 14 e2-2e 04 43 34 3a ec ec 5c	P ₇ ... P ₁₀	P ₄	P ₃ ... A ₉	G ₄ ... G ₉

- [S1]: System Deviated
Platform Alerts [P1, P2, ..., Pn]
- [S2]: System Duress
Platform Alerts [P1, P2, ..., Pn]
- [S3]: System vulnerable
Platform Alerts [P1, P2, ..., Pn]
Application Alerts [A1, A2, ..., An]
- [S4]: System Infected
Image Alerts [I1, I2, ..., In]
Grayware Alerts [G1, G2, ..., Gn]

Alert = Fn (Attribute, Constraint, Sample Rate, Recurrence, Score, weight)

The '948 patent explains that “[Figure] 7C is a block diagram illustrating a method for correlating endpoint alerts and generating endpoint warnings.”

Id. at 6:50–53.

Specifically, Figure 7C shows method 720, which “populates a risk correlation matrix 721 based upon one or more of system warning classes 722, system warnings 723, and integrity warnings 724.”

Id. at 16:29–32. The '948 patent further describes risk correlation matrix 721 as follows:

The risk correlation matrix 721 can comprise a universally unique identifier (UUID) for the system, system warnings 723 mapped to at least one system warning class 722, and at least a system warning class 722 to diagnose system deviations (i.e., system deviated integrity warnings 724), system duress, system vulnerable and system infections (i.e., system infected integrity warnings 724).

Id. at 16:38–44.

The '948 patent discloses using a configuration of event correlation matrix 633 that is analogous to the configuration of risk correlation matrix 721:

Applying qualifying rule expressions (illustrated in FIG. 7B) in the rulesets 631, integrity alerts 632 are generated and mapped to a cell in an event correlation matrix grid 633 (analogous to the risk correlation matrix 411 of FIG. 4 and grid 721 of FIG. 7C) to generate system level integrity warnings 634. The rows in the event correlation matrix 633 represent an application instance on

the device 560 (analogous to rows in the risk correlation matrix 411 that represent a device by machine identifier).

Id. at 17:22–30.

E. ILLUSTRATIVE CLAIM

Of the challenged claims, claim 1 is independent. Each of claims 2–5 depends, directly or indirectly, from claim 1. Independent claim 1 is reproduced below:

1. A method of providing real-time operational integrity of an application on a native computing environment, the method comprising:

monitoring, by a plurality of sensory inputs, one or more of network dialogs of the application, system operations initiated by the application, a runtime configuration of the application, resource utilization by the application, and integrity of the application;

generating real-time behavior based events for determining the real-time operational integrity of the application executing on the native computing environment which includes a network analyzer, an integrity processor, an event correlation matrix, a risk correlation matrix, and a trust supervisor;

correlating, by the event and risk correlation matrix, threat classifications based on the temporal sequence of the generated real-time behavior based events; and

displaying, in a plurality of runtime dashboards of an administrative console of the computing environment, real-time status indications for operational integrity of the application.

Id. at 39:32–40:11.

F. ASSERTED GROUND OF UNPATENTABILITY

Petitioner challenges the patentability of claims 1–5 of the '948 patent on the following ground (Pet. 2):

Claims Challenged	35 U.S.C. §	References/Basis
1–5	103(a) ¹	Mukherjee ² , Cooper ³

Petitioner also submits the Declaration of Seth James Nielson, Ph.D.
Ex. 1003.

II. ANALYSIS

A. LEVEL OF ORDINARY SKILL IN THE ART

Petitioner contends that an ordinarily skilled artisan for the '948 patent “would have had a bachelor’s degree in computer science, or a related field, or an equivalent technical degree or equivalent work experience, and an additional one to two years of education or experience in the field of computer security topics.” Pet. 11 (citing Ex. 1003 ¶ 88). Petitioner adds that “[m]ore education can supplement practical experience and vice versa.” *Id.* Patent Owner states that it “utilizes Petitioner’s proposed level of skill in the art.” Prelim. Resp. 11.

Based on this record, we adopt Petitioner’s articulation of the level of ordinary skill in the art, which appears to be consistent with the '948 patent and the asserted prior art, and we apply it in our analysis. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001) (the prior art, itself, can reflect appropriate level of ordinary skill in art).

¹ The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284, 287–88 (2011), revised 35 U.S.C. § 103, effective March 16, 2013. The application that resulted in the '948 patent was filed before March 16, 2013, so we apply the pre-AIA version of § 103.

² Mukherjee, et al., *Network Intrusion Detection*, IEEE Network, published May/June 1994 (Ex. 1005, “Mukherjee”).

³ Cooper, et al., U.S. Patent No. 7,451,488 B2, issued Nov. 11, 2008 (Ex. 1006, “Cooper”).

B. CLAIM INTERPRETATION

We apply the same claim construction standard used in district courts, namely that articulated in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc). *See* 37 C.F.R. § 42.100(b) (2022). In applying that standard, claim terms generally are given their ordinary and customary meaning as would have been understood by a person of ordinary skill in the art at the time of the invention and in the context of the entire patent disclosure. *Phillips*, 415 F.3d at 1312–13.

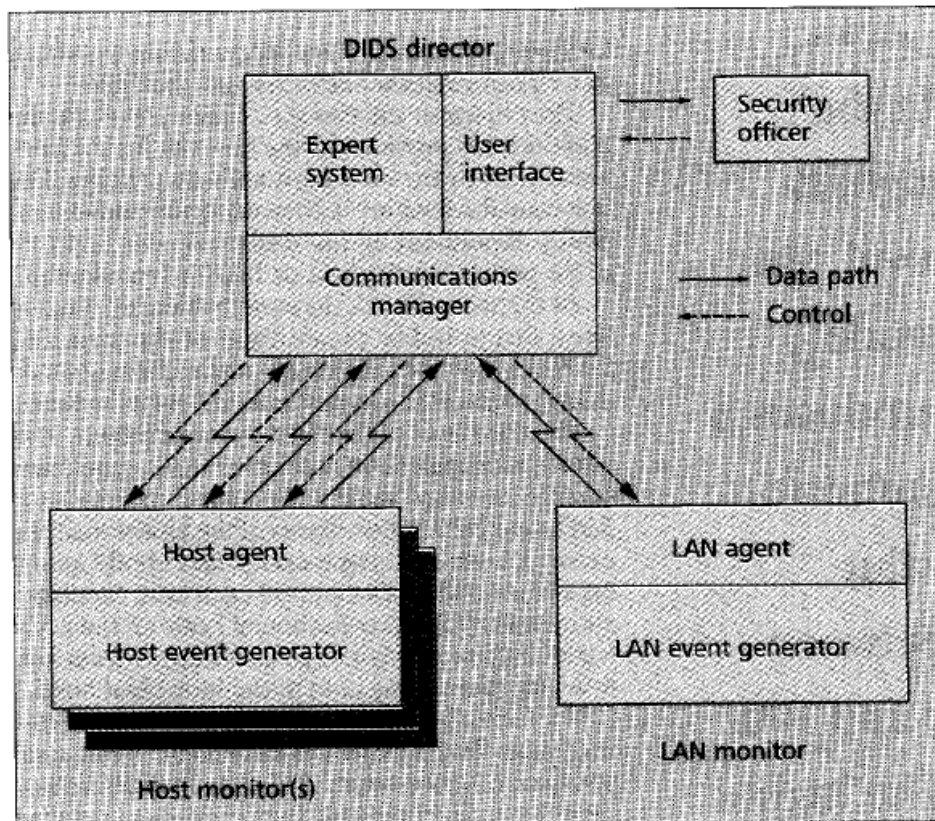
Both parties express that we do not need to construe any claim language explicitly. Pet. 11–12; Prelim. Resp. 8. Having considered the record, we agree with the parties that no explicit claim construction is necessary for this Decision. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (holding that only claim terms in controversy need to be construed, and only to the extent necessary to resolve the controversy (citing *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))).

C. ALLEGED OBVIOUSNESS OVER MUKHERJEE AND COOPER

1. *Overview of Mukherjee*

Mukherjee discloses that “[i]ntrusion detection is a new, retrofit approach for providing a sense of security in existing computers and data networks.” Ex. 1005, 1. Mukherjee discusses host-based and network-based intrusion detection systems (IDSs). *Id.* Mukherjee explains that “host-based systems employ the host operating system’s audit trails as the main source of input to detect intrusive activity,” while network-based IDSs “build their detection mechanism on monitored network traffic.” *Id.*

Mukherjee also describes a Distributed Intrusion Detection System (DIDS), which performs both host-based and network-based monitoring. *Id.* at 2, 11. Mukherjee discusses such a system in connection with Figure 2, which is reproduced below.



■ **Figure 2.** *Communications architecture.*

Figure 2 of Mukherjee depicts the communications architecture of DIDS. *Id.* at 11–12. As shown in Figure 2, the architecture includes “the DIDS director, a single host monitor per host, and a single LAN monitor for each broadcast LAN segment in the monitored network.” *Id.* at 11. “The host and LAN monitors are primarily responsible for the collection of evidence of unauthorized or suspicious activity,” and the DIDS director “is primarily responsible for its evaluation.” *Id.*

To evaluate the evidence, the DIDS director includes an expert system. *Id.* at 12. “The expert system uses rules derived from a hierarchical

Intrusion Detection Model (IDM).” *Id.* “The IDM consists of six layers, with each layer representing the result of a transformation performed on the data.” *Id.* at 12–13. At the first level, objects include audit records supplied “by the host OS, by the LAN monitor, or by any third-party auditing package,” and “all of the activity on the host or LAN is represented.” *Id.* at 13. “At the second level, the event . . . is both syntactically and semantically independent of the source standard format for events.” *Id.* The third layer “creates a subject,” which “introduces a single identification for a user across many hosts on the network.” *Id.* “The fourth layer of the model introduces the event in context.” *Id.* Mukherjee elaborates that “[t]here are two kinds of context: temporal and spatial.” *Id.* “The fifth layer of the model considers the *threats* to the network and the hosts connected to it. Events in context are combined to create threats.” *Id.* At the IDM’s top level, “the model produces a numerical value between one and 100 which represents the overall security state of the network.” *Id.*

2. *Overview of Cooper*

Cooper relates to “scanning for vulnerabilities on a continuous basis and interpreting the resulting traffic in the context of policy.” Ex. 1006, 1:21–24. Cooper describes vulnerability scanning technology that “examines the network hosts of the network by ‘probing’ or ‘scanning’ them using network traffic that is crafted to elicit a response.” *Id.* at 1:55–61. In one embodiment of Cooper’s invention, a report is generated “that associates network objects in the active policy with vulnerabilities discovered on such network objects.” *Id.* at 4:62–65.

3. *Discussion*

Petitioner argues that, in combination, Mukherjee and Cooper teach, suggest, or disclose every limitation of claims 1–5. Pet. 26–71. Petitioner

contends that “[a person having ordinary skill in the art] would have been motivated to combine Mukherjee and Cooper in part because both systems are directed towards detecting and resolving vulnerabilities in network systems.” *Id.* at 21. More specifically, according to Petitioner, “[a person having ordinary skill in the art] would have been motivated to combine Cooper’s vulnerability scans, which are designed to operate effectively with network monitoring technology, into Mukherjee’s network scanning IDS’s.” *Id.* at 22.

Patent Owner argues that “Petitioner fails to identify how certain elements of the Challenged Claims are obvious over Mukherjee in combination with Cooper.” Prelim. Resp. 1. Patent Owner faults Petitioner’s contentions regarding three of claim 1’s limitations. *Id.* at 13–19.

Having reviewed all of the parties’ arguments and evidence, we determine Petitioner does not demonstrate a reasonable likelihood of establishing unpatentability of any of claims 1–5. For the following reasons, Petitioner does not address persuasively claim 1’s recitation of “the native computing environment which includes a network analyzer, an integrity processor, *an event correlation matrix, a risk correlation matrix*, and a trust supervisor.” Ex. 1001, 40:1–4 (emphasis added).

Petitioner contends that Mukherjee discloses the claimed “event correlation matrix” and “risk correlation matrix.” Pet. 44–46 (citing Ex. 1001, 12:48–52, 14:64–65, 15:10–19; Ex. 1005, 13; Ex. 1003 ¶¶ 189–191, 195). Petitioner cites Mukherjee’s discussion of its IDM’s fourth layer as disclosing the claimed “event correlation matrix.” *Id.* at 45–46 (citing Ex. 1001, 15:10–19; Ex. 1005, 13). According to Petitioner, “[a person having ordinary skill in the art] would have understood

the Mukherjee’s description of the operation of the fourth layer of the expert model as mapping events to security issues is consistent with a ‘event correlation matrix.’” *Id.* at 46 (citing Ex. 1005, 13). Petitioner cites Mukherjee’s discussion of the IDM’s fifth layer as disclosing the claimed “risk correlation matrix.” *Id.* at 44–45 (citing Ex. 1001, 12:48–52, 14:64–65; Ex. 1005, 13; Ex. 1003 ¶¶ 189–191. According to Petitioner, “[c]onsistent with the ’948 patent’s disclosure for ‘risk correlation matrix,’ Mukherjee explains that, in the DIDS system, the fifth layer of the Intrusion Detection Model maps events (within their context produced in level four) to threats.” *Id.* at 44 (citing Ex. 1003 ¶ 190).

Patent Owner counters that “Petitioner does not show how either [Mukherjee’s] DIDS expert model’s fourth or fifth layers disclose a matrix, let alone two matrices.” Prelim. Resp. 15. Patent Owner contends that Petitioner neither shows how the operations of Mukherjee’s fourth and fifth layers correspond to a correlation, nor shows how the results Mukherjee’s operations “are equivalent to a matrix.” *Id.* Asserting that, in a related district court proceeding, “Petitioner’s real party-in-interest took a claim construction position that a ‘matrix’ has rows and columns” (*id.*), Patent Owner argues that “the Petition makes no showing that Mukherjee’s DIDS director’s expert model includes two matrices comprised of rows and columns of data” (*id.* at 15–16).

We agree with Patent Owner that Petitioner does not support sufficiently its position that Mukherjee discloses claim 1’s “event correlation matrix” and “risk correlation matrix.” Pet. 45–46. For example, when addressing the claimed “event correlation matrix,” Petitioner does not substantiate its position that Mukherjee describes “operation of the fourth layer of the expert model as *mapping* events to security issues.” Pet. 46

(emphasis added) (citing Ex. 1005, 13). Petitioner and Dr. Nielson do not identify any express disclosure of Mukherjee mapping events to security issues in its fourth layer. Ex. 1005, 13; Pet. 45–46.

Instead, Petitioner and Dr. Nielson cite Mukherjee’s disclosures of performing other actions with events in the fourth layer. For instance, Petitioner and Dr. Nielson cite Mukherjee’s disclosure that “[t]he fourth layer of the model *introduces* the event in context. There are two kinds of context: temporal and spatial.” Ex. 1005, 13 (emphasis added); Pet. 45; Ex. 1003 ¶ 187. Petitioner and Dr. Nielson also cite Mukherjee’s disclosure of “*application* of information about wall-clock time to the events [the IDM] is considering.” Ex. 1005, 13 (emphasis added); Pet. 45; Ex. 1003 ¶ 187. Additionally, Dr. Nielson cites Mukherjee’s disclosure of “*us[ing]* time windows to *correlate* events occurring in temporal proximity,” emphasizing that Mukherjee discloses certain “related patterns of behavior are also referred to as attack signatures.” Ex. 1005 (emphases added), 13; Ex. 1003 ¶ 187.

Petitioner and Dr. Nielson do not show persuasively how or why Mukherjee’s discussion of performing these other actions discloses *mapping* events to security issues. Pet. 45–46; Ex. 1003 ¶¶ 187–188. For example, Dr. Nielson’s testimony that “[a person of ordinary skill in the art] would have known that ‘attack signatures,’ in the context of IDS, refers to patterns of behavior known to be related to attacks” does not provide sufficiently objective or logical support for his conclusion that “Mukherjee discloses ‘mapping integrity warnings to endpoint events.’” Ex. 1003 ¶ 188. Nor does Dr. Nielson’s other testimony. *Id.* ¶¶ 187–188.

Moreover, even if Petitioner had substantiated its position that Mukherjee describes mapping events to security issues in the fourth layer,

that contention and Petitioner’s other arguments and evidence do not provide a sufficiently persuasive, objective basis for characterizing Mukherjee’s fourth *layer* as the claimed “matrix.” Pet. 45–46. Indeed, as Patent Owner notes, in a related district court proceeding, Petitioner’s real party-in-interest has taken the position that the ’948 patent’s claimed “event correlation matrix” requires “rows or columns.” Ex. 2003, 1, 178; Prelim. Resp. 8–9, 15–16; Pet. 73. Yet, neither Petitioner nor Dr. Nielson states, much less substantiates, that Mukherjee’s fourth layer includes rows or columns. Pet. 45–46; Ex. 1003 ¶¶ 186–188.

In much the same way that Petitioner does not support its position that Mukherjee discloses the claimed “event correlation matrix,” Petitioner does not support its position that Mukherjee discloses the claimed “risk correlation matrix.” Pet. 44–45. For example, Petitioner does not provide a sufficiently persuasive, objective basis for asserting that Mukherjee’s fifth *layer* constitutes the claimed “matrix.” *Id.*

For the foregoing reasons, Petitioner does not demonstrate a reasonable likelihood of prevailing on its assertion that claim 1 would have been obvious over Mukherjee and Cooper. Additionally, Petitioner’s arguments and evidence regarding dependent claims 2–5 do not cure the foregoing deficiencies in the challenge to independent claim 1. Pet. 59–71. Accordingly, Petitioner does not demonstrate a reasonable likelihood of establishing unpatentability of any of the challenged claims.

III. CONCLUSION

Because we determine that the information presented in the record does not establish there is a reasonable likelihood that Petitioner would prevail with respect to at least one challenged claim of the patent ’948 patent, we do not institute an *inter partes* review.

IV. ORDER

For the reasons given, it is:

ORDERED that the Petition is *denied*, and no trial is instituted.

IPR2023-00800
Patent 8,990,948 B2

FOR PETITIONER:

Robert Hansen
Scott Amankwatia
THE MARBURY LAW GROUP, PLLC
bhansen@marburylaw.com
samankwatia@marburylaw.com

FOR PATENT OWNER:

Peter Lambrianakos
Vincent Rubino
Joseph Mercadante
FABRICANT LLP
plambrianakos@fabricantllp.com
vrubino@fabricantllp.com
jmercadante@fabricantllp.com